

## Theory Problems:

### Problem 1:

In order to make sure that the group is in fact a group with the modulo multiplication operator it must have the following traits: Closure, Associativity, Identity, and Inverse.

Closure is met because any operation done between any two element in  $Z_{18}$  will yield an Element in  $Z_{18}$

Associativity is because reordering the parenthesis in the operation will yeild the same operation  
example being  $(a+b)+c = a+(b+c)$

Identity element is met because for multiplatication because the elements of the set are only needed to be multiplied by one so the elements of the set will be unchanged

Inverse element is not met because every element in the set does not have a multiplicative inverse

### Problem 2:

In order to make sure that the group is in fact a group with the  $\gcd(.)$  operation it must have the following traits: Closure, Associativity, Identity, and Inverse.

Closure is met because any operation done between any two element in  $\gcd(.)$  will yield an Element in  $\gcd(.)$

Associativity is because reordering the parenthesis in the operation will yeild the same operation  
example being  $(a+b)+c = a+(b+c)$

Identity element is met because for multiplatication because the elements of the set are only needed to be multiplied by one so the elements of the set will be unchanged

Inverse element is not met because every element in the set does not have an inverse

Problem 3:

The GCD of the 2 numbers 19838 and 10946 is 26

$$19838 \% 10946 = 8892$$

$$10946 \% 8892 = 2054$$

$$8892 \% 2054 = 676$$

$$2054 \% 676 = 26$$

```
10946 % 19838 =  
10946  
19838 % 10946 =  
8892  
10946 % 8892 =  
2054  
8892 % 2054 =  
676  
2054 % 676 =  
26  
676 % 26 =  
0
```

Problem 4:

4.)  $\mathbb{Z}_{35}$  19

$$\begin{aligned} \gcd(35, 19) &: 19 = 1 \times 19 + 0 \times 35 \\ \gcd(19, 16) &: 16 = -1 \times 19 + 1 \times 35 \\ \gcd(16, 3) &: 3 = 1 \times 19 - 1 \times 16 \\ &= 1 \times 19 - 1 \times (1 \times 35 - 1 \times 19) \\ \gcd(3, 1) &: 1 = 2 \times 19 - 1 \times 35 \\ \gcd(3, 1) &: 1 = (1 \times 16) - (5 \times 3) \\ &= (1 \times 16) - 5(2 \times 19 - 1 \times 35) \\ 35 - 17 &= (24) &= 1 \times 16 - 10 \times 19 + 5 \times 35 \\ &= -1 \times 19 + 1 \times 35 - 10 \times 19 + 5 \times 35 \\ &= -11 \times 19 + 6 \times 35 \\ &11 + 6 = 17 \end{aligned}$$

Problem 5:

5.) a.)  $6x \equiv 3 \pmod{23}$

$$6x \pmod{23} = 3$$

$$6x \pmod{23} = 1 \quad x = 4$$

$$6x = 1 \pmod{23}$$

$$\Rightarrow 3 \pmod{23} \quad x = 12$$

b.)  $7x \equiv 11 \pmod{13}$

$$7x \pmod{13} = 11$$

$$7x \pmod{13} = 1 \quad x = 2$$

$$7x \pmod{13} = 11 \quad x = 22$$

$$22 \pmod{13} = x = 9$$

c.)  $5x \equiv 7 \pmod{11}$

$$5x \pmod{11} = 7$$

$$5x \pmod{11} = 1, \quad x = 9$$

$$5x \pmod{11} = 63 \pmod{11} = 9$$

$$x = 8$$

$$x = 2$$

Programming Question: For this assignment we utilize the code for multiplicative inverse given to us by the professor.